nehta

eHealth

eHealth Clinician's Desktop User Guide

For General Practice

Release 1 for: Healthcare Identifiers and Clinical Document (CDA) Viewing

Final

Version 1.0 – July 2012

National E-Health Transition Authority

REQUEST FOR FEEDBACK

NEHTA requests feedback on this User Guide to assist with its further development.

Please email **eHealthUG.enquiries@nehta.gov.au** to:

1. Provide feedback on the document
2. Receive updates on further developments and releases
3. Ensure you have the latest version

ACKNOWLEDGEMENT

The author thanks the following people who contributed to the development of this Guide:

Dr John Aloizos AM (NEHTA Clinical Lead Sponsor)
Ms Niesje Hees (NEHTA Manager)
Ms Arlynne Asuncion (NEHTA Analyst)

Ms Barbara Allen
Mr Matt Antcliff
Mr Mitchell Burger
Ms Joanne Carroll
Dr Lynne Davies
Dr Peter Del Fante
Dr Gary Frydman
Ms Judy Evans
Ms Jo-Anne Hammersley
Mr Roger Hewitt
Ms Tracey Johnson
Mr Peter Makris
Ms Cheryl McCoy
Ms Heather McDonald
Mr John McMillan
Ms Lorinda Panton
Ms Deepa Patole
Dr Nathan Pinskier
Mr John Siemers
Mr Gary Smith
Mr Micah Starkis
Dr Jeff Urquhart
Ms Anna Maree Yip

Author: Jeff Parker, JP Consulting (Aust) Pty Ltd. www.jpconsulting.com.au
filename: eHealth Clinician's Desktop User Guide R1 GP - FINAL v1.0.docx

National E-Health Transition Authority Ltd

Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.

www.nehta.gov.au

Disclaimer

NEHTA makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. NEHTA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Security

The content of this document is confidential. The information contained herein must only be used for the purpose for which it is supplied and must not be disclosed other than explicitly agreed in writing with NEHTA.

Copyright ©2012, NEHTA.

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

TABLE OF CONTENTS

1 Introduction 4
1.1 Intended Audience 4
1.2 Purpose 4
1.3 Scope and Environment of This User Guide 4
1.4 Structure 6
1.5 Important Note 6
1.6 Related Key Information Resources 7

2 User Guide Context 8
2.1 New eHealth Features – Current and Future 8
2.1.1 Healthcare Identifiers 9
2.1.2 Clinical Document (CDA) Viewing 10
2.2 Benefits to your Practice 11
2.2.1 Broad Benefits from Participating in eHealth 12
2.2.2 Meeting Practice and Governance Requirements 12
2.2.3 Patient, Practitioner and Practice Benefits 13
2.2.4 Realisable Benefits for Your Practice 14

3 Implementation, Verification and Meaningful Use 16
3.1 Purpose and Introduction 16
3.2 Clinical Governance and eHealth 16
3.2.1 Focus on Clinical Care Outcomes, not Technology 17
3.2.2 Data Sharing and Improving the Care Continuum 17
3.2.3 Clinical Governance Elements and Processes 18
3.3 Quality Improvement and eHealth 18
3.3.1 Include eHealth in Quality Improvement 19
3.3.2 Accurate and Complete Data is Necessary 20
3.3.3 Improving Data Quality and Practice Performance 21
3.3.4 Implementing Healthcare Identifiers is an Essential Prerequisite 22
3.4 Preparations Required for Healthcare Identifiers 22
3.4.1 Organisational Entities and HPI-Os 23
3.4.2 HPI-O Clinical and Business Uses 23
3.4.3 HPI-O Structure Options 25
3.4.4 Deciding on Your HPI-O Structure 26
3.4.5 Roles and Access for the HI Service 27
3.4.6 Setting Up Your User Roles and HPI-O 28
3.4.7 Linking Clinicians and Authorised Staff to Your HPI-O 29
3.5 Implementing Healthcare Identifiers 30
3.5.1 Adding IHIs to Patient Records 30
3.5.2 The Status of IHIs 32
3.5.3 Options for Downloading IHIs 33
3.6 Verifying Correct Operation 33
3.6.1 Healthcare Identifiers 34
3.6.2 Clinical Document (CDA) Viewing 35
3.7 Achieving Meaningful Use 36

4 Checklists for HI Usage 37
4.1 For Front-Desk and Practice Administration Roles 37
4.2 For GPs and Other Clinicians 38

5 Further Information and Support 39

6 Acronyms and Abbreviations 40

1 Introduction

1.1 Intended Audience

This Clinician's eHealth[1] Desktop User Guide (User Guide) is intended for General Practices:

- GPs, practice nurses, practice managers and staff of those general practices who will be upgrading their Desktop Software to a version that supports new eHealth functionality[2] as it is released; and
- Medicare Locals, Divisions of General Practice and other organisations that provide support to general practices in the implementation and use of eHealth.

1.2 Purpose

This guide is intended to assist you and your practice to:

- Understand the new eHealth features that are now available in the recent update to your Desktop Software, and how the features will be beneficial;
- Identify the work process, organisational and governance changes that may be necessary in your practice so that you can benefit from the new features;
- Understand the prerequisites for the implementation and use of the new eHealth features, and undertake the necessary once-off pre-implementation set up steps;
- Verify that your implementation of the new features operates correctly; and
- Gain initial and ongoing value from the use of the new eHealth features through a quick reference checklist and access to education and support resources.

1.3 Scope and Environment of This User Guide

The National E-Health Transition Authority (NEHTA[3]) has contracted with GP Desktop Software vendors to incorporate a number of key national eHealth specifications[4] into commonly used software products, with a view to supporting the eHealth Site projects[5] that are being funded by the Australian Government. In the near future, these products and others that also conform to the specifications will be available more broadly in general practices across Australia.

[1] eHealth is defined by the World Health Organisation as being the "combined use of electronic communications and information technology in the health sector".

[2] The e-Health functionality referred to is as outlined in the Australian Government's e-Health Program. See http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/theme-ehealth for details.

[3] See http://www.nehta.gov.au

[4] One of NEHTA's roles is to develop specifications and standards for e-Health that are to be implemented in the Australian healthcare system. This requires modifications to software used by healthcare providers.

[5] These are projects that received funding to be early adopters of e-Health. The list of projects is available at: http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/ehealth-sites

Conformance to those national eHealth specifications is required for products to interact electronically with the new eHealth features. The process for this is explained later in section 3.6. **You should contact your Desktop Software vendor to see if they are including the new eHealth features into their products and to understand the extent of their conformance with the specifications.**

This version of the User Guide is applicable for general practices and covers the following currently available eHealth functionality that is built into conformant Desktop Software:

- Healthcare Identifiers; and
- Clinical Document (CDA[6]) Viewing.

Further versions of the User Guide will be developed to align with future releases of NEHTA specified eHealth functionality (listed below), and for other community-based healthcare professionals, e.g. private specialists and allied health professionals.

The national eHealth program will enable the delivery over time of major new nationally agreed standards based eHealth services such as:

- Shared Health Summaries, Event Summaries, and access to the national personally controlled electronic health (eHealth) record system;
- Secure Message Delivery, and improved security, including e-Signatures;
- e-Referrals, e-Discharge Summaries, and e-Specialist Letters;
- e-Medication Management, including Electronic Transfer of Prescriptions and improvements to e-Prescribing; and
- e-Diagnostic Services, including e-Requesting and e-Reporting for pathology and diagnostic imaging.

For your practice to use the above eHealth functions as they become available, your Desktop Software vendor needs to update their products to be conformant with the relevant national eHealth specifications and standards as they are released. This process includes participation in a testing regime.

You can be kept up to date with national eHealth program developments by subscribing to receive update emails at **http://www.yourhealth.gov.au/subscribe**

By following this guide, your practice, clinicians and nominated staff will become registered with and be able to use the main initial new eHealth feature, i.e. the Healthcare Identifiers Service, and be able to effectively utilise further eHealth functionality as it becomes available.

This User Guide should be read in conjunction with your software vendor's release notes, and implementation and user guides, which will provide relevant product-specific information. This material should be included with the software update kit provided by your vendor, or available from their web-site.

[6] CDA stands for Clinical Document Architecture, which is a standard for defining electronic versions of documents such as referrals, discharge summaries, etc.

1.4 Structure

The User Guide has three main components, which align with the chapters that follow:

1. User Guide Context – overviews the new eHealth features, explains why your practice might undertake to use them, and what benefits you should reasonably expect;

2. Implementation, Verification and Meaningful Use – outlines what you need to do to implement the new eHealth features and how to verify their correct implementation and operation – the goal being to achieve meaningful use of the new features for those clinical transactions conducted by your practice that the new eHealth features support; and

3. Checklist – a quick reference list of key information and instructions for your efficient use of the new eHealth features, including links to further information and who to contact if you need advice or assistance.

1.5 Important Note

This guide does not replace the advice, guidance and support provided by your software vendor. As the guide is generic (i.e. applicable to all upgraded GP Desktop Software products) there will be instances where additional important information will be provided by your vendor.

The new eHealth features will include the ability for your practice to share clinical patient data electronically (inbound and outbound), possibly for the first time. As with all eHealth systems there is a small risk of unintended consequences if not implemented and operated correctly. This risk should be lower than at present as the new healthcare identifiers will act as a key to correctly match patient, practitioner and practice data.

In addition, as the new eHealth features require your practice's computer systems to access external online services via the Internet, if not done already, you should also:

- Review the IT security arrangements in your practice and take action to address any shortcomings or areas of risk[7]; and

- Review the reliability and performance of your practice's internet connection and consider upgrading if warranted.

It is recommended that you seek advice and support from your Software Vendor or other organisation that provides you with IT and/or eHealth support. Your Medicare Local (or Division of General Practice if still in existence) may also be able to provide assistance or services to support implementing the new eHealth features in your practice. See chapter 5 for links to web-sites and other useful information related to obtaining advice and support.

[7] See the RACGP's Computer and Information Security Standards (CISS) at http://www.racgp.org.au/ehealth/ciss

1.6 Related Key Information Resources

The following is a list of information resources that you may find useful for introductory or other reference purposes on eHealth generally and on the national eHealth program specifically. It is not essential that you read through all of these at this point in time, as many are referred to later in the guide itself.

Australian Government's web-sites, which have information, including brochures, on eHealth, and the ability to subscribe for updates and notification of key events.	http://www.ehealth.gov.au http://www.ehealthinfo.gov.au http://www.yourheatlh.gov.au
Introduction to the eHealth record system for healthcare professionals	http://publiclearning.ehealth.gov.au/modules/hcpIntro/index.html – a Learning Module
Department of Health and Ageing's web-site on eHealth.	http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth
Healthcare Identifiers Act 2010	http://www.comlaw.gov.au/Details/C2010C00440
Healthcare Identifiers (Consequential Amendments) Act 2010	http://www.comlaw.gov.au/Details/C2010A00073
Healthcare Identifiers Regulations 2010	http://www.comlaw.gov.au/Details/F2010L01829
DHS[8] web-site for healthcare providers. Includes information and resources about the HI Service.	http://www.medicareaustralia.gov.au/provider/ http://www.medicareaustralia.gov.au/provider/health-identifier/
DHS web-site for individuals	http://www.humanservices.gov.au/customer/services/medicare/healthcare-identifiers-service
RACGP's eHealth web-site. Includes resources on clinical governance, quality improvement and computer security.	http://www.racgp.org.au/ehealth
AGPN's eHealth web-site. Note: AGPN to transition to Australian Medicare Local Network from 1 July 2012.	http://agpn.com.au/programs/ehealth-and-information-management
The AMA's Guide to Using the PCEHR (Draft available).	Draft is available at http://ama.com.au/node/7648
The eHealthAus YouTube Channel that includes videos demonstrating many features and benefits of eHealth.	http://www.youtube.com/user/eHealthAus
NEHTA web-site for Healthcare Identifiers.	http://www.nehta.gov.au/connecting-australia/healthcare-identifiers
The NEHTA Model Healthcare Community web-site. Includes a video that shows how the Healthcare Identifier Service will work.	http://www.nehta.gov.au/connecting-australia/healthcare-identifiers/discover-the-model-healthcare-community

[8] DHS: The Commonwealth Department of Human Services, formally known as Medicare Australia

2 User Guide Context

2.1 New eHealth Features – Current and Future

The latest update to your GP Desktop Software includes access to the following eHealth capabilities[9]:

Currently available eHealth functions
• Healthcare Identifiers • Clinical Document (CDA) Viewing

The above capabilities, which are described in the following sections, are the initial set from a broader suite of eHealth features that you should expect to see included in updates from your software vendor over time.

Subsequent product releases are expected to expand to encompass the following comprehensive set of eHealth features:

Electronic documents and records	Underlying eHealth services
• e-Referral • e-Specialist Letter • e-Discharge Summary • Shared Health Summary • Event Summary • eHealth record system (ability to upload and share electronic health record documents) • e-Medication Management, including Electronic Transfer of Prescriptions and improved e-Prescribing • e-Diagnostic Services, including e-Requesting and e-Reporting for pathology and diagnostic imaging	• Healthcare Identifiers • Clinical Document (CDA) Viewing • Secure Message Delivery (SMD) • NASH (authentication and security), including e-Signatures • Assisted Consumer Registration • Clinical Terminology Standards

Note that the features included in this current update, i.e. Healthcare Identifiers and Clinical Document (CDA) Viewing, are essential prerequisites for the future new eHealth features. As such it is recommended that you implement this current update as outlined in this guide in a timely manner so that implementation of the future updates will be as straight forward as possible for your practice.

The suite of eHealth solutions and services being released over time:

- Is included in your Desktop Software product by its vendor in collaboration with NEHTA and DHS; and

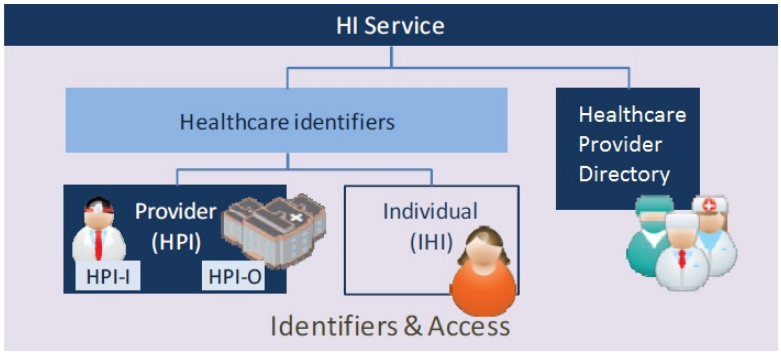
[9] Note that some software vendors may include additional e-Health-related functionality in their updated products, and also enhancements and bug fixes to the product itself. Please check the release notes that came with the software update.

- Is subject to testing to ensure conformance with national eHealth standards and specifications (this is described later in section 3.6).

The above eHealth features can be used in your practice progressively as they are included in updates to your Desktop Software vendor's product. Implementing the updates as they are released should make it easier for you to extend to include use of the eHealth record system into your practice, should you choose to. You should find this approach better than attempting to implement the features all in one step at a later time.

2.1.1 Healthcare Identifiers

The Healthcare Identifiers (HI) Service is a national system for uniquely identifying healthcare professionals, organisations and individual consumers of healthcare services. The service is operated by DHS. Healthcare Identifiers will help ensure individuals and healthcare professionals can have confidence that the right information is associated with the right individual at the point of care.



The HI Service allocates and manages the following types of healthcare identifiers:

- **Healthcare Provider Identifier – Individual (HPI-I)** – for healthcare professionals involved in providing patient care;

- **Healthcare Provider Identifier – Organisation (HPI-O)** – for organisations that deliver healthcare (such as general practices or hospitals); and

- **Individual Healthcare Identifier (IHI)** – for individuals receiving healthcare services[10].

In addition, there is the Contracted Service Provider (CSP) Registration Number, which is for organisations that Healthcare Providers may contract with for IT-related services so that they may use or disclose healthcare identifiers in the course of providing their services. [11]

Healthcare Identifiers can only be used for the purposes described in the Healthcare Identifiers Act 2010 and Healthcare Identifiers Regulations 2010 (see section 1.6for links), including, for example, for electronic referrals, discharge summaries and medication management.

[10] Note that all Australians have already been assigned an IHI. IHIs do not replace Medicare or DVA numbers and they do not affect the way medical benefits are claimed.

[11] A Contracted Service Provider (CSP) does not receive a healthcare identifier but a registration number. A CSP must be authorised by a healthcare organisation to transact with the HI Service.

The use of HPI-Is and HPI-Os in your practice requires that certain IT-related security measures be in place, namely PKI Certificates. This requirement is discussed later in this document.

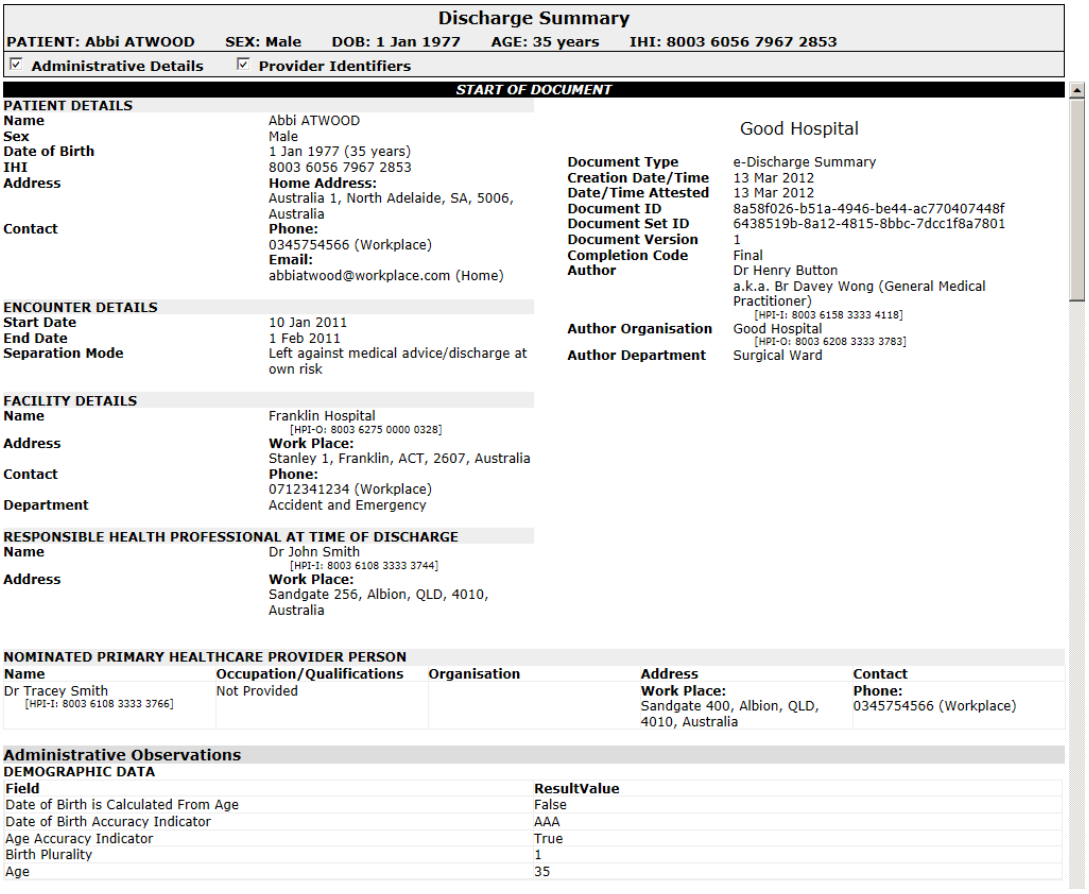
An important component of the HI Service is the **Healthcare Provider Directory (HPD)**, which is a consent-based listing of healthcare providers (individuals and organisations) registered with the HI Service. It includes contact and location details, as well as details of services provided. Once a healthcare provider is registered with the HI Service, they can choose to be listed in the HPD and nominate what information can be published. The HPD is not a public directory and is only available to healthcare providers and authorised users (explained later in section 3.4.5) of organisations registered with the HI Service.

It is advantageous for your practice and clinicians to be listed and linked in the HPD so they can be found (from searches performed by other healthcare providers) and selected for referrals and other forms of secure electronic communications. Clinicians need to consent that their HPI-I is visible in the HPD and also for it to be linked to your practice's HPI-O. This can be done on the DHS HPOS web-site, which is discussed later.

Over time the HPD is intended to become the primary source for healthcare provider contact and service information for eHealth purposes, so it is important that information in it is accurate and kept up to date.

2.1.2 Clinical Document (CDA) Viewing

The ability to display CDA compliant clinical documents, such as e-Discharge Summaries, has been included in the latest version of your Desktop Software. An example of the initial part of a CDA compliant e-Discharge Summary is shown below.



Discharge Summary

PATIENT: Abbi ATWOOD **SEX: Male** **DOB: 1 Jan 1977** **AGE: 35 years** **IHI: 8003 6056 7967 2853**

☑ **Administrative Details** ☑ **Provider Identifiers**

START OF DOCUMENT

PATIENT DETAILS

Name	Abbi ATWOOD
Sex	Male
Date of Birth	1 Jan 1977 (35 years)
IHI	8003 6056 7967 2853
Address	**Home Address:** Australia 1, North Adelaide, SA, 5006, Australia
Contact	**Phone:** 0345754566 (Workplace) **Email:** abbiatwood@workplace.com (Home)

Good Hospital

Document Type	e-Discharge Summary
Creation Date/Time	13 Mar 2012
Date/Time Attested	13 Mar 2012
Document ID	8a58f026-b51a-4946-be44-ac770407448f
Document Set ID	6438519b-8a12-4815-8bbc-7dcc1f8a7801
Document Version	1
Completion Code	Final
Author	Dr Henry Button a.k.a. Br Davey Wong (General Medical Practitioner) [HPI-I: 8003 6158 3333 4118]
Author Organisation	Good Hospital [HPI-O: 8003 6208 3333 3783]
Author Department	Surgical Ward

ENCOUNTER DETAILS

Start Date	10 Jan 2011
End Date	1 Feb 2011
Separation Mode	Left against medical advice/discharge at own risk

FACILITY DETAILS

Name	Franklin Hospital [HPI-O: 8003 6275 0000 0328]
Address	**Work Place:** Stanley 1, Franklin, ACT, 2607, Australia
Contact	**Phone:** 0712341234 (Workplace)
Department	Accident and Emergency

RESPONSIBLE HEALTH PROFESSIONAL AT TIME OF DISCHARGE

Name	Dr John Smith [HPI-I: 8003 6108 3333 3744]
Address	**Work Place:** Sandgate 256, Albion, QLD, 4010, Australia

NOMINATED PRIMARY HEALTHCARE PROVIDER PERSON

Name	Occupation/Qualifications	Organisation	Address	Contact
Dr Tracey Smith [HPI-I: 8003 6108 3333 3766]	Not Provided		**Work Place:** Sandgate 400, Albion, QLD, 4010, Australia	**Phone:** 0345754566 (Workplace)

Administrative Observations

DEMOGRAPHIC DATA

Field	ResultValue
Date of Birth is Calculated From Age	False
Date of Birth Accuracy Indicator	AAA
Age Accuracy Indicator	True
Birth Plurality	1
Age	35

It is possible that your practice is currently receiving discharge summaries and other clinical documents electronically, e.g. specialist letters, and also sending electronic referrals. It is also possible, but unlikely, that these will be CDA compliant, unless your messaging provider's service is also conformant with NEHTA's Secure Message Delivery (SMD) specifications. Using eHealth software and services that are conformant with NEHTA specifications is mandatory for organisations to be able to participate in the national eHealth system.

At this stage the ability to send CDA compliant documents is limited. However, your software now has the capability to view these documents, which will be beneficial as they become more widely available over time. As healthcare organisations gain the ability to create and send CDA documents, (e.g. hospital discharge summaries) they will need to work with their community of healthcare providers, e.g. GPs, to ensure that these are implemented safely and correctly.

Please consult your software vendor's documentation for advice on how to use this feature.

2.2 Benefits to your Practice

There is a broad range of potential benefits to be achieved from the effective use and progressive uptake of eHealth. The key areas of benefits include:

- Improving your practice's ability to comply with practice standards and requirements for patient safety, risk minimisation and quality improvement (e.g. for accreditation);

- Providing an opportunity for your practice to strengthen its clinical governance arrangements and interact more effectively with other healthcare organisations and practitioners involved in the care of your patients; and

- Creating efficiencies and cost savings for your practice when implemented competently, including when business processes are designed to take optimal advantage of the new eHealth functionality.

Achieving benefits from the use of the new eHealth features in your practice is progressive in nature, i.e. it starts off low and grows as you and other healthcare providers use more and more of the features.

The benefits also won't just occur on their own, e.g. from simply installing and configuring the software. It is likely that changes in work practices and other organisational and business aspects will be required in order to achieve what you should reasonably expect. This is discussed in the chapter that follows.

Implementing this initial set of eHealth features in effect starts your practice on the eHealth pathway. It provides an opportunity to establish accurate patient, practitioner and practice identification information in your computer systems. This is an imperative for data quality and integrity (also known as data cleansing), which is essential for quality improvement activities and improved practice performance. The implementation of Healthcare Identifiers in your practice is also an essential prerequisite for the implementation of future eHealth features.

The information that follows outlines the types of benefits that you should reasonably expect from the implementation of the broader suite of eHealth features over time.

2.2.1 Broad Benefits from Participating in eHealth

The Australian Government's eHealth program aims to provide you and your practice with the following:

- More timely access to accurate and more comprehensive information about your patients, including their medical history and treatment, i.e. creating less reliance on patients' memories;
- Quick and efficient sharing of patient information between peers, for example between a GP and a specialist;
- More time treating patients, less time spent tracking down records and test results;
- Faster access to relevant information, helping you make better clinical decisions and spend more time on patient care;
- Access to potentially life-saving patient information in an emergency situation;
- Online tools designed to help patients, including those with chronic and complex conditions, better manage their health; and
- Synergies and a critical mass of participating healthcare organisations to create a more connected healthcare system, which will ensure better continuity and coordination of care.

2.2.2 Meeting Practice and Governance Requirements

To the maximum extent possible, this User Guide aligns with and aims to support your practice's use of the new eHealth features in meeting the relevant requirements of organisations such as the Australian Commission on Safety and Quality in Healthcare (ACSQHC)[12] and the Royal Australian College of General Practitioners (RACGP)[13]. This includes in the areas of:

1. Governance for safety and quality in health service (integrated systems of governance to actively manage patient safety and quality risks);
2. Patient Identification (including data quality and matching with DHS, etc.);
3. Clinical Handover (including referrals, handling discharge summaries, etc.);
4. Quality improvement using Practice Data (including increasing focus on the clinical safety, risk management and quality improvement aspects of Clinical Governance);

[12] See ASCQHC – Governance for Safety and Quality in Health Service Organisations: http://www.safetyandquality.gov.au/internet/safety/publishing.nsf/Content/F8B0A43F125B45E5CA25796C007DE677/$File/Standard%201.pdf

[13] See RACGP Standards for General Practices 4th edition http://www.racgp.org.au/standards, and Appendix B - Clinical Governance: http://www.racgp.org.au/standards/appendixb

5. Managing patient information to support preventative care (including standardised coding of conditions, use of Shared Health Summaries, etc.); and

6. Secure and consistent electronic communication and the move to less paper (including addressing privacy, security and confidentiality concerns).

This User Guide and the initial release of the new eHealth features supports item 1 above and specifically addresses item 2. The introduction of the Healthcare Identifiers is fundamental to supporting patient identification requirements (e.g. as outlined in RACGP Standard 3.1, Criterion 3.1.4[14]), and is a critical first step in introducing the foundation services for eHealth in Australia.

Subsequent releases of software with additional eHealth functionality will enable your practice to more comprehensively comply with the broader set of practice requirements, and achieve the expected benefits over time.

2.2.3 Patient, Practitioner and Practice Benefits

Through their support of technical and practice standards, the new eHealth features, when implemented and used effectively, should provide your practice and patients with a range of benefits. In broad terms these include:

For e-Referrals, Specialist Letters and e-Discharge Summaries

- Improved accuracy of demographic information via healthcare identifiers, promoting the rapid identification of patients, providers and services, minimising duplicate records and accelerating decisive information exchanges
- Improved accuracy of clinical information via secure and structured communications between referrers (e.g. general practitioners) and referees (e.g. specialists), promoting safety, error reduction and reduced duplication of clinical and administrative effort
- Improved cost-efficiencies via increasing interoperability of practices and systems, with a corresponding decrease in miscommunication, duplication of testing and associated risks
- Improved coordination of services and treatments, from diagnosis to interventions, leading to improved continuity of care and increasingly integrated care

For Shared Health Summaries, Event Summaries and the eHealth Record System

- Improved decision making through access to patient clinical history that is shared for any clinician providing ongoing care for a patient (with the patient's consent), thus avoiding full reliance on the patient's memory
- Ability to validate rather than recapture patient's medical history. Improved delivery of multi-disciplinary care for patients with complex needs – supports a team based system of healthcare delivery
- Particular advantages for updating relevant clinical information for Aboriginal and Torres Strait Islander peoples, mobile populations and for patients who do not have a regular GP
- Significant benefits for gaining information about un-referred patients who often get lost in the system and for whom information about clinical events are sometimes not captured

[14] Amongst other things, this standard states "Correct patient identification is vital for patient safety and the maintenance of patient confidentiality."

The electronic exchange and sharing of patient documents and reports between healthcare providers will ultimately lead to improved safety and quality, through the exchange of timely, accurate and structured information, enabling better patient outcomes.

The timing of the availability of the above eHealth features, and hence the start of the flow of benefits, is expected in the initial stages of the national eHealth program, i.e. commencing in July 2012.

In addition, the following eHealth features are expected to be available sometime after July 2012, and are dependent upon further specifications, development and the completion of policy and regulatory activities. The subsequent eHealth features and their expected benefits are outlined below.

For e-Medication Management, including Electronic Transfer of Prescriptions and improved e-Prescribing

- Prescribers can avoid hand-signing prescriptions through the use of electronic signatures, and thus obtain savings in the use of paper, printing and the time involved
- Reduced potential for errors of transcription and/or interpretation, leading to improved health outcomes through lower dispensing error rates
- Electronic prescriptions will allow more flexibility and convenience for the consumer (e.g. the existing need for consumers to re-visit their prescriber to have lost prescriptions re-issued can be avoided in many instances)
- Build a technical foundation for improvements in the quality and safety of medication management

For E-Diagnostic Services, including e-Requesting and e-Reporting for pathology and diagnostic imaging

- Allow practices to receive and access diagnostic reports electronically with increased confidence that the test results are linked to the right patient and care provider
- Save further time by not having to match diagnostic result reports with requests
- Reduced unnecessary test orders by clinicians due to improved access to diagnostic information
- Reduce the chances of mis-matching when results are received
- Increased confidence that previous results can be matched to the correct person and be included when producing cumulative reports
- Save time by reducing the need to investigate status of requests and reports

2.2.4 Realisable Benefits for Your Practice

When implemented successfully and used effectively, the new eHealth features can provide significant benefits to your practice. As an example, the benefits of secure messaging include:[15]

- Fast message delivery and reduced handling. Traditionally mail is opened, sorted, placed into a GP's mail-box, read/actioned, and sent to a nurse or receptionist for action or scanning; and often sits in the scanning pile for 2-3 days. This process is subject to delays, data losses and is less organised than secure messaging.

[15] Adapted from "General Practice Cost/Benefits Analysis for Using Secure Messaging", South East Alliance of General Practice, 2008; and also see Medical Observer 16 March 2012, page 5, *Secure messaging switch could save practices $30,000 to offset PCEHR* article

Secure messages are read and actioned by a GP, and incorporated into the practice's electronic record. The sender, through the software they use, also receives notification of message receipt or delivery failure;

- Reliable message delivery. Reduces resending of information, duplication of effort, and wasted time in chasing up receipt of documents/referrals; and

- Improved clinical data management, which reduces clinical errors and directly contributes to better patient care. It is much easier to transfer more comprehensive clinical information to the other health care professionals involved in the patients care, directly improving the level of patient care through a better informed care team.

These benefits can result in savings for practices that implement secure messaging for incoming and outgoing communications (and other related eHealth features) from such changes as:

- Reduced faxes sent, stationary used, stamps/postage, staff handling and follow-up phone calls;

- Reduced staff time spent keying in data, scanning, filing and retrieving paper documents;

- Increased efficiency in creating clinical documents and reports, as key clinical data is available electronically; and

- More data available electronically, providing improved data searching and patient record interrogation for recalls, reminders, service design, etc.

A benefit from the implementation of NEHTA's Secure Message Delivery (SMD) specifications is that healthcare providers will be able to exchange messages with other healthcare providers who use a messaging service provider that is also SMD-compliant[16]. This standardisation will make exchanging messages as easy and as ubiquitous as emailing, but with dramatically higher levels of security and reliability.

In addition, as healthcare providers have access to better information and can therefore amend their provision of healthcare to produce better outcomes, the risk of adverse outcomes is expected to reduce and with that comes a reduction in exposure to medico-legal liability.

[16] Note that existing messaging providers will need to update their software to be SMD-compliant

3 Implementation, Verification and Meaningful Use

3.1 Purpose and Introduction

This section of the User Guide provides you and your practice with guidance on:

- How to identify the work process, organisational and governance changes necessary to make most effective use of the new eHealth features included in the updated Desktop Software you use;
- How to implement and verify that the new eHealth features work properly in your practice, in the context of your clinical and business usage of the Desktop Software used in your practice; and
- How to access further information and assistance related to your use of the new eHealth features.

Note that you will need to refer to the installation guide and release notes (and any other provided documentation) received from the vendor of the software you use for specific instructions related to the installation, set up and operation of their product, including how it relates to the new eHealth features. As previously suggested, you should seek expert assistance in implementing the software update.

This chapter focusses specifically on the new Healthcare Identifiers (HI) functionality included in your updated Desktop Software. Implementing HI in your practice is a critical initial step in your eHealth journey that is important to get right. The chapter also discusses broader topics and issues that you need to be aware of and do something about in order to obtain optimum benefits from your participation in the new eHealth environment.

3.2 Clinical Governance and eHealth

Clinical governance covers areas such as patient safety, risk management and quality improvement. It refers to the set of relationships and responsibilities established by a healthcare service between its executive, workforce (clinical and non-clinical) and stakeholders (including consumers). It provides a system through which clinicians and managers are jointly accountable for patient safety and quality care. The purpose of clinical governance is the promotion of safety and quality which eHealth, in addition to other capabilities in your practice, can improve.

The Australian Commission on Safety and Quality in Health Care describes a model of governance in Standard 1 in their National Safety and Quality Health Service Standards[17] that includes both corporate and clinical governance, where corporate governance provides a

[17] See ACSQHC – Governance for Safety and Quality in Health Service Organisations: http://www.safetyandquality.gov.au/internet/safety/publishing.nsf/Content/F8B0A43F125B45E5CA25796C007DE677/$File/Standard%201.pdf; and
ACSQHC – National Safety and Quality Health Service Standards Sept 2011: http://www.safetyandquality.gov.au/internet/safety/publishing.nsf/Content/NationalSafetyAndQualityHealthServiceStandards

structure through which corporate objectives (e.g. social, fiscal, legal and human resources) are set and achieved, and performance is monitored.

In order to meet the requirements for this and other key standards, including those of the RACGP (Standards for General Practice 4th edition – Appendix B – Clinical Governance[18]), practices require, amongst other things, good business processes, good information systems and good data. Implementing eHealth as outlined in this guide supports these requirements.

3.2.1 Focus on Clinical Care Outcomes, not Technology

The eHealth literature repeatedly recommends and/or appeals to those implementing eHealth to focus on improving patient outcomes rather than implementing technology for its own sake. A clinical governance framework for eHealth in your practice should be established with a mandate to provide oversight, monitoring and support for the implementation of eHealth deliverables that impact clinical care and patient outcomes.

Use of the new eHealth features (including the eHealth record system) will sharpen the focus on increased clinical safety risks and data governance issues due to increased reliance on the successful integration of health information systems and information sharing models – both for improved clinical service delivery and collaborative quality improvement activities. The absence of good clinical governance may create risks where eHealth systems could incorrectly focus on what can be done technologically and not prioritise innovations that are most relevant to enhancing patient care.

3.2.2 Data Sharing and Improving the Care Continuum

A key benefit of eHealth's incorporation into clinical governance is that it will address fragmentation across primary and acute sectors, thus strengthening the coordination and integration of patient care processes across organisational boundaries.

At a practice level, the introduction of eHealth and the eHealth record system may for the first time involve practices sharing patient and clinical information electronically with other healthcare providers. This needs to be done in a way that minimises risks related to safety.

The importance of ensuring patient safety and the medico-legal protection of your practice cannot be overstated. Data shared by your practice to others and data you receive from other healthcare organisations will usually be depended upon for clinical decision making.[19]

Hence, this User Guide strongly suggests, as part of your practice's planning for eHealth, that you design and implement effective clinical governance arrangements – both within your practice and in how your practice "connects" with other local and/or regional healthcare organisations for the safe sharing of patient information.

[18] See http://www.racgp.org.au/standards/appendixb; and
http://www.racgp.org.au/standards/313; and
http://www.racgp.org.au/afp/201004/201004steer.pdf

[19] Note also, as previously mentioned in section 1.5, you should implement the RACGP's Computer Information Security Standards (CISS) to maximise the protection of your practice's data and information systems.

3.2.3 Clinical Governance Elements and Processes

In developing a clinical governance framework for your practice, the following elements and processes, which have an impact on clinical utility, clinical effectiveness and clinical safety, would need to be considered from an eHealth point of view:

- Consumer input and engagement (patient focused)
- Clinical safety of products and programs being introduced
- Effectiveness (fit for purpose)
- Data quality and its governance
- Appropriateness of the outcomes to patient care and appropriateness of the interventions being delivered
- Clinical risk management including adverse event reporting
- Complaints management
- Workforce training and enablement
- Measurement of benefits, performance and progress (measures will include core, enablers and interim outcome measures)
- Continuous quality improvement including lessons learnt, barriers and enablers

Organisations that can provide direct advice and support in the design and implementation of clinical governance arrangements include:

- The RACGP;
- The ACSQHC;
- Your Medicare Local / Division of General Practice; and
- Your Local Health Network (LHN).

In addition, the AMA, with assistance from NEHTA, has published a document entitled *Guide to Medical Practitioners on the use of the Personally Controlled Electronic Health Record System*[20], which includes excellent guidance related to policies and protocols that would be valuable input for the development of a clinical governance arrangement for your practice. It also includes discussion on medico-legal considerations.

3.3 Quality Improvement and eHealth

Key requirements of an effective approach to quality improvement, within the context of clinical governance, include:

- The collection and analysis of performance data (clinical and organisational);

- The implementation of strategies for performance improvement, including for adverse event prevention, based on evidence; and

- A patient clinical record that allows for the systematic audit of the contents against those Standards that the practice is required to comply with.

[20] See http://ama.com.au/node/7648 for a draft version of their guide that is released for consultation

3.3.1 Include eHealth in Quality Improvement

Improving your practice's clinical and organisational performance can be greatly enhanced through incorporating a deliberate focus on eHealth in your Quality Improvement activities.

One approach for this that has proved successful is the eCollaborative model[21], which is being implemented jointly by NEHTA and the Improvement Foundation[22]. The eCollaborative model promotes the following change principles (copied from its web-site) that position eHealth as an essential component for quality improvement.

In reading these principles and considering their implementation in your practice, remember that the eHealth features in the current release of your Desktop Software, i.e. Healthcare Identifiers and Clinical Document (CDA) Viewing, are essential prerequisites for the eHealth record system and other subsequent eHealth functions.

eCollaborative Change Principles

1. Build and Maintain the Team
   - Set realistic goals
   - Communicate with other team members
   - Engage the team
   - Assign roles and responsibilities
   - Reflect on and review what you are doing

2. Undertake foundational work for the eHealth record system
   - Obtain a healthcare provider identifier for individual health professionals (e.g. general practitioners, registered nurses and Aboriginal health workers) (HPI-I)
   - Obtain a healthcare provider identifier for your organisation (HPI-O)
   - Obtain a patients' individual healthcare identifier (IHI)

3. Develop systems to improve and maintain data quality across your clinical system
   - Archive inactive and deceased patients' records
   - Use consistent disease coding
   - Develop a practice policy to ensure that patient's current problem and past history diagnoses are reviewed regularly
   - Record results in the right place, including pathology results with HL7[23]
   - Use your clinical software or compatible data extraction tool to improve data quality
   - Develop systems to maintain data quality, particularly for medications, allergies and immunisations lists

4. Develop systems to support the Shared Health Summary (SHS)
   - Use process mapping to identify opportunities to integrate the SHS into the general practice and health service work flow
   - Decide and document the nominated provider(s) responsible for maintaining the currency and accuracy of the SHS
   - Inform your practice team about the processes of uploading a SHS
   - Develop policies and procedures for the checking, uploading and maintaining a SHS

5. Engage your patients in the eHealth record system
   - Identify patients who would most benefit from a SHS
   - Inform your patients about the eHealth record system and, in particular, the SHS
   - Develop systems to obtain informed consent from identified patients
   - Process map the points of care at which patients can input into their SHS

[21] See http://www.ecollaborative.com.au

[22] See http://www.improve.org.au

[23] HL7 is a standard for the structure of electronic healthcare messages. See http://www.hl7.org

- Design processes to increase patient review of their SHS
- Develop policies about points of care when patients are prompted to review their SHS
- Develop process for patients to advise of any changes to their medication lists
- Seek patient advice on how they can contribute to the development and maintenance of their SHS

6. Develop systems to improve the integration of care through use of the Shared Health Summary across the care team
   - Communicate with your local providers concerning the SHS
   - Develop ways to use the SHS with other members of the patient's care team
   - Develop processes that include the SHS in team care arrangements, Home Medicine Reviews, mental health plans, referrals to Emergency, specialists and allied health providers
   - Explore tools and resources to share care plans electronically
   - Engage the patient to develop new strategies for sharing their SHS across their care team

7. Develop systems and processes to improve patient self-management skills using the eHealth record system
   - Use the eHealth record system to improve health literacy and self-efficacy
   - Ensure the whole team is aware of and able to access the eHealth record system to enhance patient self-management skills
   - Develop key messages and terminology that support the reinforcement of key self-management concepts by the team
   - Explore patients' use of the eHealth record system
   - Use the eHealth record system to promote other online health resources
   - Bring patients together to provide feedback about the eHealth record system and how its use can be improved

3.3.2 Accurate and Complete Data is Necessary

Item 2 in the list above clearly positions Healthcare Identifiers as essential early steps in the eHealth and quality improvement journey. Having accurate and complete patient identification data in your information systems is an essential prerequisite for eHealth. Other prerequisites include identification data for practice clinicians and staff, and your practice organisation.

In addition, the Shared Health Summary (SHS) is also identified as a critical component of the eHealth record system[24]. Maintained by a patient's usual practice or health service (as declared by the patient as their Nominated Provider), the SHS will be a "clinically reviewed" summary of your patient's health status.

To achieve improved performance and to participate in eHealth your practice will need (when the eHealth SHS functionality becomes available) to produce health summaries that are *safe to share*, i.e. your practice will need to maintain accurate and current allergy reports, medication lists, immunisation records and medical histories for most if not all of your active patients.

[24] The fields within a Shared Health Summary are congruent with the RACGP standards for health summaries. This will enable easy extraction of Shared Health Summaries from local clinical systems into the eHealth record system.

The following points outline the important relationship between data quality in your practice and the effective use of eHealth:

- **Accurate and complete** patient identification/demographic information is required in your practice's clinical records system **before patient IHIs can be included, and**;
    - The correct IHI is required **before patient clinical information can be shared** via the eHealth features; and
- **Accurate and complete** clinician, staff and organisation identification information is required for your HPI-Is and HPI-O(s), **and**;
    - These must be established correctly also **before patient clinical information can be shared**.

Accurate and complete patient clinical information is required in your systems for the **safe sharing** of health summaries and other clinical documents, e.g. e-Referrals, etc. This includes to the eHealth record system when it becomes available (subject to consent and access controls established by consumers).

As discussed earlier, there can be serious consequences to your patients and practice from the sharing (outgoing and incoming) of incomplete and inaccurate data.

3.3.3 Improving Data Quality and Practice Performance

With support from NEHTA, both Pen Computing Systems (PCS) and the Canning Division of General Practice have developed a simple to use tool to help assess, analyse and improve the quality of data contained within most Desktop Software systems for general practice.

The Clinical Data Self-Assessment (CDSA) Tool combines the functionality and capabilities of the Pen Clinical Audit Tool (CAT)[25] and the Canning Data Extraction Tool[26] to allow users to interrogate general practice clinical desktop software and provide a report on data completeness and quality.

The CDSA Tool works with most of the popular GP Desktop Software products and provides general practice with the following functionality:

- Report on completeness of patient demographic and heath summary data within the clinical system;
- Report on duplicate patient records within the clinical system;
- Provide a 'dashboard' or traffic light report to general practice on data quality status and improvements which can be made over time; and
- Provide guidance on addressing identified gaps and improving overall clinical data quality.

NEHTA has made both versions of the CDSA Tool available for free use until March 2013. For current licence holders, be sure to download the latest software update to access the CDSA functionality.

[25] See http://www.clinicalaudit.com.au/

[26] See http://www.canningdivision.com.au/dataextraction.html

For non-licence holders, you can download:

- The Canning Tool from http://www.canningdivision.com.au/dataextraction.html; or
- The Pen CAT tool from http://install.pencs.com.au/clickonce/clinicalaudit/publish.htm (user Username cdsa, and Password cdsa1234 when asked).

User guides and release notes are available for both versions. For more information about how to improve your data quality using these tools, contact your Medicare Local or your Division of General Practice, including for advice on the potential ongoing costs involved.

3.3.4 Implementing Healthcare Identifiers is an Essential Prerequisite

It is clear from the above that preparing for and implementing Healthcare Identifiers in your practice is a top priority as it is an essential prerequisite for the implementation and use of subsequent eHealth functionality, i.e. none of it can be used without Healthcare Identifiers. In addition, implementing Healthcare Identifiers in your practice effectively will further improve the quality of your data and also enable improvements in your practice's performance.

The rest of this chapter:

- Focusses on options for you to consider in the implementation of Healthcare Identifiers;
- Provides guidance on approaches to their implementation; and
- Includes suggestions on how you can verify they are working in your practice.

3.4 Preparations Required for Healthcare Identifiers

This section outlines actions you need to take BEFORE installing the software update and utilising the Healthcare Identifier features. In summary this includes, in order:

- Deciding on a structure for your practice organisation's HPI-O(s), including staff Roles, and then applying for them and having them set up, including of any necessary security mechanisms, e.g. Organisation PKI certificates; and
- Associating clinicians' HPI-Is and setting up access for nominated staff with your organisation (HPI-O), and setting up any necessary Individual PKI certificates, which your clinicians will need to apply for. OMOs and ROs may also need to apply for PKI certificates if they wish to utilise the HI service admin functions in HPOS (see section 3.4.5 for definitions of OMO and RO).

DHS has a web-site that contains useful information, guides and forms for the HI Service at: http://www.medicareaustralia.gov.au/provider/health-identifier/.

In particular, the following document is recommended introductory reading:

Healthcare Identifiers Service information guide – Introduction and overview, at: http://www.medicareaustralia.gov.au/provider/health-identifier/files/4820e-introduction-and-overview.pdf

In addition, there are a number of informative brochures available at: http://ehealthinfo.gov.au/brochures, where you can also order printed versions if you prefer.

You may find it beneficial to talk about the setting up of Healthcare Identifiers for your practice with the organisation(s) that provide you with IT and/or eHealth support, as it can be complex depending on your organisational structure and level of knowledge and experience.

3.4.1 Organisational Entities and HPI-Os

A Healthcare Provider Identifier – Organisation (HPI-O) is an identifier for use by a healthcare provider organisation and is a prerequisite for participation in the national eHealth system. The *Healthcare Identifiers Act 2010*[27] defines a healthcare provider organisation as:

> *... an entity, or a part of an entity, that has conducted, conducts or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).*

To participate in the HI Service, healthcare provider organisations must register for a HPI-O with the HI Service Operator (currently DHS). Organisations that are eligible for an HPI-O must meet the following requirements:

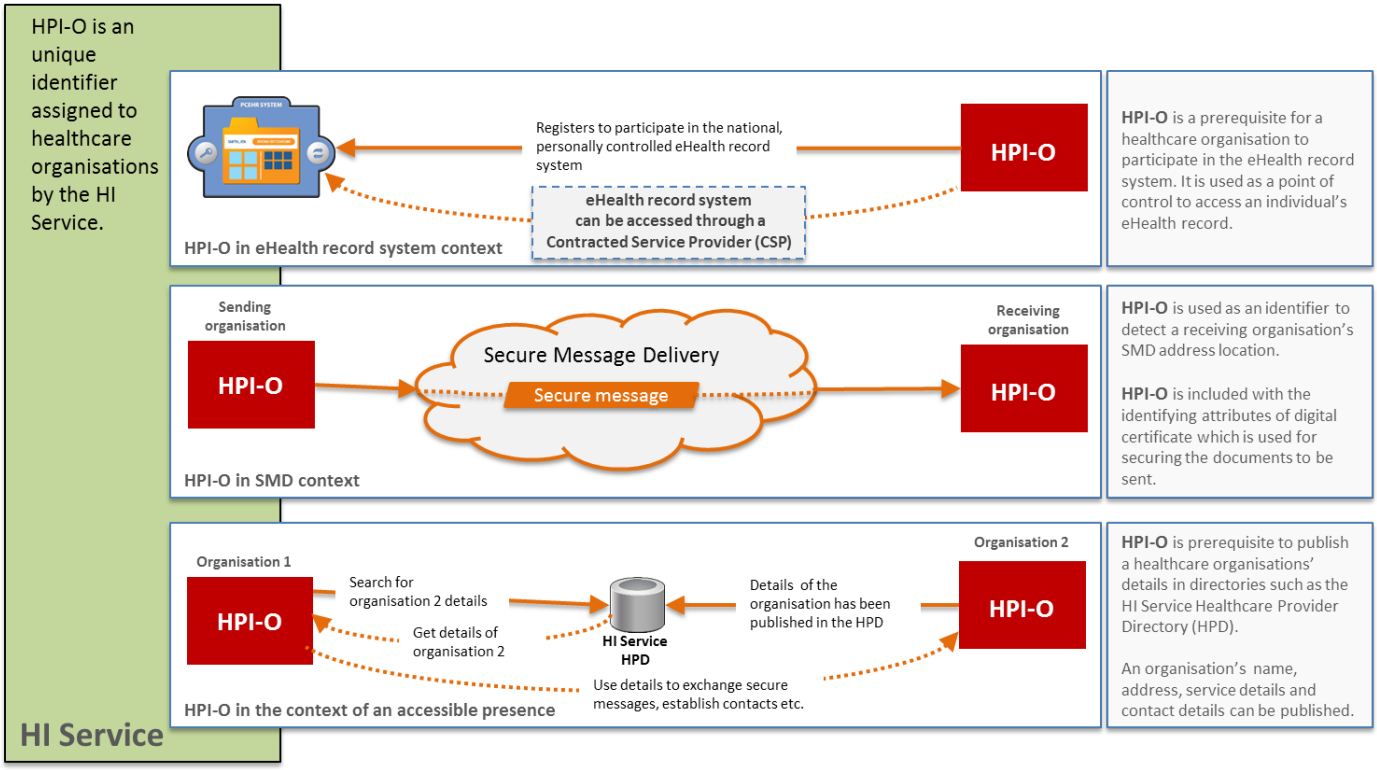
- Provide a healthcare service;
- Be a legal entity; and
- Employ or contract one or more individual healthcare providers or sole traders who are employed for the purpose of providing a health service.

3.4.2 HPI-O Clinical and Business Uses

HPI-Os play important roles in different aspects of eHealth, and it is important that you understand these so that your practice's needs can be properly addressed in setting up your HPI-O configuration.

The diagram below illustrates that your practice needs a HPI-O to interact with the HI Service, eHealth record system, Secure Message Delivery (SMD) and the Healthcare Provider Directory (HPD).

[27] Healthcare Identifiers Act 2010, Act No. 72 of 2010 as amended, 1 July 2011; See table in section 1.6 for internet link. Note also Section 9a, subclause 3.


HPI-O is an unique identifier assigned to healthcare organisations by the HI Service.
Registers to participate in the national, personally controlled eHealth record system
HPI-O
eHealth record system can be accessed through a Contracted Service Provider (CSP)
HPI-O in eHealth record system context
HPI-O is a prerequisite for a healthcare organisation to participate in the eHealth record system. It is used as a point of control to access an individual's eHealth record.
Sending organisation
HPI-O
Secure Message Delivery
Secure message
Receiving organisation
HPI-O
HPI-O in SMD context
HPI-O is used as an identifier to detect a receiving organisation's SMD address location.
HPI-O is included with the identifying attributes of digital certificate which is used for securing the documents to be sent.
Organisation 1
HPI-O
Search for organisation 2 details
Get details of organisation 2
HI Service HPD
Details of the organisation has been published in the HPD
Organisation 2
HPI-O
Use details to exchange secure messages, establish contacts etc.
HPI-O in the context of an accessible presence
HPI-O is prerequisite to publish a healthcare organisations' details in directories such as the HI Service Healthcare Provider Directory (HPD).
An organisation's name, address, service details and contact details can be published.
HI Service

The key points from this diagram are:

- The same HPI-O may be used for HI Service access, eHealth record system access, providing contact information of your practice organisation in the HPD, and as a reference for a location for secure messaging;

- Alternatively, using Network HPI-Os (discussed in the next section), you may establish a separate HPI-O for each of the following, or a HPI-O for a combination of the following, to:

    - Participate in the HI Service;
    - Identify the sender/receiver for secure messaging;
    - Provide a point of control for access for the eHealth record system and alignment with consent processes to meet patient eHealth record privacy needs; and
    - Provide contact information of your practice that can be published in the HPD;

    The considerations related to the above approach are discussed below in section 3.4.4.

- For Secure Message Delivery (SMD), the HPI-O is an identifier used to locate the electronic address and the associated digital certificate for the transmission of secure messages to your practice organisation; and

- A record of your practice's HPI-O will be retained by the eHealth record system and the HI Service when they are accessed, for audit purposes as prescribed in the legislation.

There are also other uses of HPI-Os, such as for identification of an organisation in discharge summaries and referrals, and for the alignment of credentials for use with the National Authentication Service for Health (NASH) when it is implemented.

The above points introduce important considerations for you in determining how you design the HPI-O structure for your practice. Further elaboration of these key considerations is provided in the following sections.

3.4.3 HPI-O Structure Options

There are two organisation types that can be registered within the HI Service:

- Seed Organisation – identified as **Seed HPI-O**; and
- Network Organisation – identified as **Network HPI-O**.

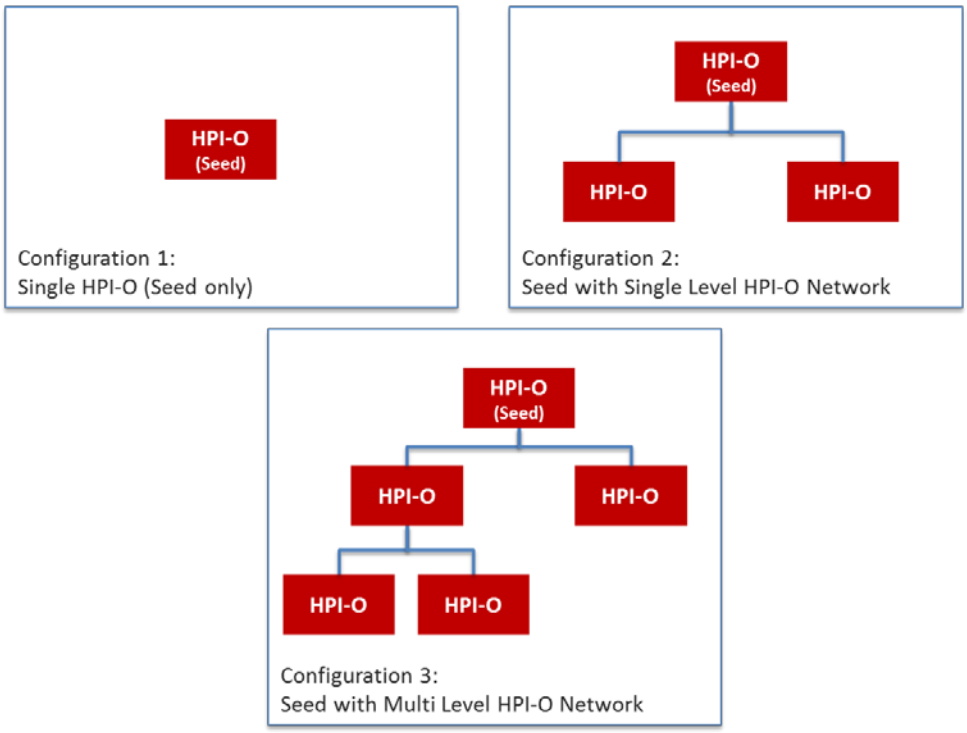
A healthcare provider organisation that participates in the HI Service could have:

- A configuration of one Seed HPI-O; or
- A Seed HPI-O with one or more Network HPI-Os under the Seed HPI-O.

A **Seed HPI-O** is a legal entity within Australia that provides or controls the delivery of healthcare services.

A **Network HPI-O** is a healthcare provider organisation that provides services as part of the Seed HPI-O. It can be registered in order to identify a business area or function within the Seed HPI-O and can be linked to either a Seed or another Network HPI-O.

The types of HPI-O structures that are possible are illustrated in the diagram below.



In order to avoid undue complexity, this User Guide does not provide guidance for practice organisations that have an arrangement with a CSP (Contracted Service Provider). Such practice organisations would be aware of this and the contracted service provider would liaise with the practice organisation to design and bring into effect the most suitable HPI-O configuration.

3.4.4 Deciding on Your HPI-O Structure

As introduced in section 3.4.2 above, choosing an appropriate HPI-O configuration is an important factor that influences your practice organisation's participation in:

- The Healthcare Identifier (HI) Service;
- The eHealth Record System;
- Secure Message Delivery (SMD); and
- The Healthcare Provider Directory (HPD).

In most cases in general practice, the most suitable HPI-O configuration will be the simplest, i.e. just a Seed HPI-O – Configuration 1 in the above diagram.

However, practice organisations that have multiple sites and/or business units, e.g. clinics, pharmacies, etc. that operate separately as part of an over-arching organisational or corporate structure, will likely require a different configuration, i.e. a Seed HPI-O and one or more Network HPI-Os under that, and potentially Network HPI-Os under other Network HPI-Os, as illustrated in the above diagram in the other Configurations.

In addition to organisational or corporate structure considerations, some factors that may influence you in determining an appropriate HPI-O configuration include:

- Whether you have or need separate endpoints[28] for secure messaging. If so, a separate Network HPI-O may be required for each;

- Whether you need separate control points for accessing the eHealth record system, e.g. for within separate business units from the rest of the practice organisation, e.g. clinics. If so, separate Network HPI-O(s) may be required;

- If there is a need to specifically audit access to the HI Service or the eHealth record system for separate business units. If so, it may be appropriate to set up Network HPI-O(s) for that purpose; and

- If a presence in the Healthcare Provider Directory (HPD) is required for separate organisational or business units, e.g. clinics. If so, Network HPI-O(s) may be required.

The HI Service also enables eHealth record access to the Network HPI-Os beneath the nominated Network HPI-O in the structure, i.e. access cascades downwards from the HPI-O authorised by the patient, be it the Seed or a Network HPI-O. This method used to control eHealth record access may also factor into your considerations for structuring HPI-Os in your practice organisation.

If you feel that your practice organisation requires more than the simple configuration of just a Seed HPI-O, then it is recommended that you seek advice, and if necessary assistance, from the organisations listed in chapter 5.

[28] Endpoints for secure messaging are organisational locations or business units that you require to be defined with their own identity for receiving and/or sending SMD-compliant messages.

The rest of this User Guide contains useful information for all types of practice organisations, although it is intended to provide guidance to those who have decided on the configuration of just having a Seed HPI-O.

3.4.5 Roles and Access for the HI Service

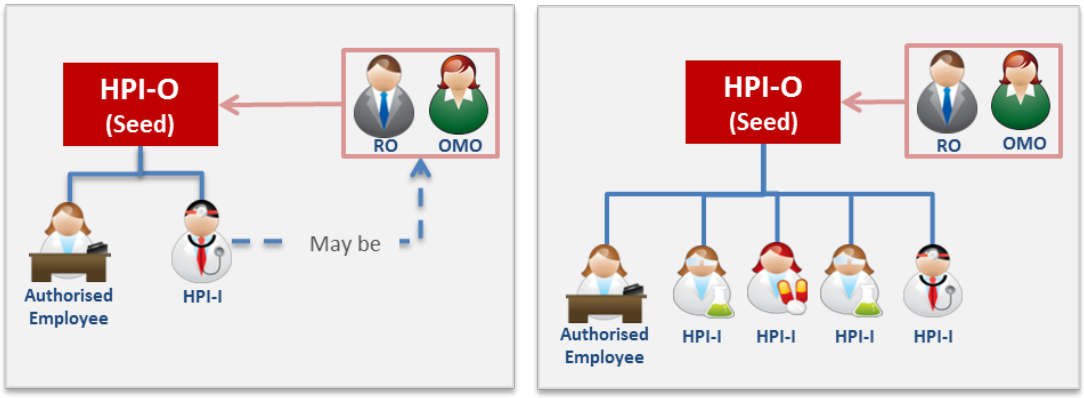
Roles in the HI Service have been designed for use by individual healthcare providers and employees of healthcare organisations. These roles have been developed so that appropriate access to the system can be assigned for each type of use.

To use the HI Service an authorised user must be in one (or more) of the following roles.[29]

- Responsible officer (RO) – the officer of an organisation who accepts responsibility for the participation of their organisation in the HI Service (sometimes also called the Public Officer), which may be the Practice Principal;
- Organisation maintenance officer (OMO) – the officer(s) of an organisation who accepts responsibility for maintaining information about their organisation within the HI Service (sometimes also called the Organisation Maintenance Role – OMR), which may be the Practice Manager, if you have one, and/or other senior staff;
- Authorised employee – an individual within an organisation who requires access to IHI records and provider identifiers to assist with patient administration; and
- Individual healthcare provider – a health professional who provides healthcare services to the general public, who has an HPI-I and may have an Individual PKI certificate (discussed below).

Note that these roles are not mutually exclusive. An individual person may be assigned to one, some or all of them. The DHS HI web-site has Information Guides available for each of the above roles at http://www.medicareaustralia.gov.au/provider/health-identifier/

The diagram below illustrates how these roles might be set up for a single HPI-O practice configuration.



Users can only access the HI Service with strictly controlled access credentials to perform their duties in the service. Functions they are able to perform depend on their role(s). These

[29] Information in this section is drawn from the DHS document "Healthcare Identifiers Service information guide – Introduction and overview", referred to earlier.

credentials ensure that each user is able to access the HI Service with a high degree of security and information protection. There are two types of credentials that are used by the HI Service:

- An Individual Authentication Token or Individual Public Key Infrastructure (PKI). This token is a physical device[30] required by ROs, OMOs and individual healthcare providers to access the HI Service; and

- An Organisation Authentication Certificate or Organisation PKI (sometimes also called a Location PKI). This certificate is a software module required by an organisation accessing the HI Service that interacts with your Desktop Software.

Once an authorised user (i.e. individual healthcare provider, RO, or OMO) has their access credentials, they can access the HI Service securely through their software system if it is compatible with the HI Service, or using DHS's Health Professional Online Services (HPOS) web-site.

3.4.6 Setting Up Your User Roles and HPI-O

The process to assign people to the roles introduced above and set up your HPI-O is described and is conducted on the DHS HI Service web-site[31]. There are forms that will need to be completed and sent in, depending on some pre-conditions related to how your practice organisation and staff are currently "known" to DHS. It is likely that Evidence of Identification documentation will need to be provided to DHS as part of this process.

The process can be comparatively straight forward if your practice organisation is currently registered for the Medicare Online Claiming Services (e.g. for online billing), in which case:

- The Organisation PKI currently used for Medicare Online can be used for the HI Service, but it will need to be HI-enabled (discussed below);

- The person set up as your practice's Duly Authorised Officer (DAO) for your Organisation PKI certificate could be set up as the Responsible Officer (RO) for the HI Service; and

- You may choose to set up your RO also as your practice's OMO.

The above approach is not mandatory and you may choose a different approach, but in the majority of cases in general practice, this may be the most appropriate.

Your DAO would also already have access to the DHS HPOS web-site, in which a number of the set up actions can be conducted – the most significant being to enable your existing Organisation PKI for the HI Service (they will have been set up as an OMO for the seed organisation).

[30] This may be a USB stick or a Smart Card that contains the relevant PKI certificate

[31] See http://www.medicareaustralia.gov.au/provider/health-identifier/

The DHS web-site has an online user guide that demonstrates how to perform the actions necessary to complete the set up process. It is available at:

http://www.medicareaustralia.gov.au/hpos/online-user-guides/hi/

If you choose a different approach to that discussed above, then relevant information and the requirements and processes are outlined in the above web-site. You may also find it beneficial to contact the DHS HI Service help desk and/or your Medicare Local's eHealth Support Officer for advice and assistance – see chapter 5.

3.4.7 Linking Clinicians and Authorised Staff to Your HPI-O

In addition to the steps above, it will also be necessary to link the HPI-Is of doctors and other clinicians working at your practice with the practice's HPI-O. Required steps are:

- Clinicians should have their HPI-I from correspondence sent to them from AHPRA[32], or they can obtain it from the AHPRA web-site (**http://www.ahpra.gov.au/**) using their login account, or by contacting DHS;

- Clinicians need to be registered as individual healthcare providers with the HI Service. GPs are registered and accredited through AHPRA along with thirteen other clinician types[33]. If your clinicians are not eligible for registration with AHPRA, they may be eligible to register with the HI Service through contacting DHS;

- While not mandatory, it is also strongly recommended that clinicians in your practice:
  - Have their own Individual PKI Certificate; and
  - Set the flag on their HPI-I profile that enables them to be visible in the Healthcare Provider Directory (HPD). This can be done on the HPOS web-site (**http://www.medicareaustralia.gov.au/hpos/**) or by contacting DHS); and

- Your practice's OMO, through the HPOS web-site, can then link the HPI-Is of clinicians working in your practice with your HPI-O. The process for this, which includes obtaining consent from clinicians to link to their HPI-I, is also explained in the online user guide referred to above.

In addition to clinicians, your OMO may also set up staff at your practice as Authorised Employees in the HI Service. This role is intended for staff, e.g. including those at reception, who are responsible for making sure patient identification information in your Desktop Software is correct, up to date and has an IHI assigned to it. This is discussed in the following section.

Note that ROs/OMOs have certain responsibilities under the HI Act (e.g. must understand the responsibilities of maintaining a register of individuals or identifying them appropriately in transmissions).

These staff do not require an Individual PKI, and instead access the HI Service with your practice's Organisation PKI through your Desktop Software with its embedded HI functionality.

[32] Australian Health Practitioner Regulation Agency

[33] Currently ten provider types are eligible for AHPRA registration and accreditation. From 1 July 2012 this will expand to include another four provider types bring the total to fourteen.

The process for setting up Authorised Employees is also described in the online user guide on the DHS web-site, as referred to above.

3.5 Implementing Healthcare Identifiers

Now that you have decided upon and established the necessary Roles, your practice's HPI-O and the links to it in the HI Service for your clinicians and nominated staff, you can plan and then implement the update to your Desktop Software that includes the Healthcare Identifiers functionality.

The documentation that came with the software update will outline how you should go about doing this for the particular Desktop Software product that you use. If you have any questions or concerns regarding installing the update, then please be sure to contact the vendor of the product. As each product is different, this User Guide does not provide product-specific guidance.

After you have installed the update, there are a number of things it is suggested you then do:

- Firstly, your updated Desktop Software will most likely have a feature to record a clinician's HPI-I with their profile or address book entry. In most cases this will need to be manually typed in. The HPI-I needs to be stored this way as it is needed for clinicians to perform eHealth functions that require access to the HI Service, which is something they will all do.

- Secondly, you'll need to decide on an approach to adding patient IHIs to your practice's patient records system by downloading them from the HI Service. This is discussed in the following section.

In addition, if not already done in your practice, you should consider:

- Designing an approach and commence reviewing and improving the quality of the clinical data stored in your systems about your patients. This should be done generally as part of good clinical practice, and importantly also in preparation for your practice's participation in eHealth – as discussed in section 3.3 above; and

- Implementing and/or participating in a clinical governance arrangement that can enhance your practice's ability to deal with clinical safety risks and data governance, and importantly "connect" your practice more effectively with other healthcare providers involved in your patient's care – as discussed in section 3.2 above.

3.5.1 Adding IHIs to Patient Records

When the above steps are complete and your software is configured to suit, you will be able to commence downloading your patients' IHIs from the HI Service and having them stored in your Desktop Software system. However, before you do this it is suggested that you review and where needed correct data stored in your practice information systems. Particular focus on data related to patient demographics is suggested.[34]

[34] See section 3.3.3 for information about tools that can assist with this process

Data cleansing of patient identification information held in your systems should be undertaken on a regular basis in order to ensure a more accurate match with data held in the HI Service.

When an attempt to download an IHI is made in your Desktop Software, the software and the HI Service compares the following data fields:

- Surname (mandatory)
- Date of Birth (mandatory)
- Gender (mandatory)
- Given Name
- Medicare or DVA number
- Address

Note: the items marked as mandatory must be present in your system to conduct an IHI search. The others are optional, however at least additionally using the patient's Medicare or DVA number will result in improved match results.

Note too that it is mandatory to have a combination of Medicare / DVA number and first name (or Address and first name, if Medicare / DVA number is not supplied).

It is essential that data in your practice information system match **exactly** with data on the patient's Medicare card and in the HI Service. If there is an error on even one item, then the attempt to download the IHI will fail. The HI Service is purposely designed to notify only that the attempt has failed and not to advise of which data fields are correct and which are incorrect. This feature is present to prevent fraudulent searching of IHIs, e.g. to address concerns of identity theft.

If present, you will also need to resolve duplicate records for the same patient before attempting to match records with the HI Service. Your Desktop Software should indicate to you if duplicate patient records exist and not allow the allocation of the same IHI to more than one record. This is a requirement of the software that NEHTA has mandated.

Some common issues that have been identified through initial trials at a number of locations include failures to match with IHI records as a consequence of errors in the patient's:

- Medicare number and IRN or DVA number;
- Surname and/or Given name(s), including, for example, the inclusion of multiple names (or initials) in data fields intended to have only single names;
- Address, e.g. including mixing up street and postal addresses;
- Date of birth; and
- Gender.

By improving patient identification data stored in your Desktop Software system staff can increase match rates when searching for patients' IHIs and the associated data in the HI Service. It has been observed that more recent patient information (less than 2 years old) will result in greater likelihood of a match.

It is possible that a patient's data held in the HI Service is incorrect, for example if they have changed address, in which case you will need to ask your patient to contact DHS to have the data corrected.

If it is not possible to download a patient's IHI, then this does not affect in anyway their ability to receive care or anything related to their payment arrangements. It just means your

practice won't be able to include eHealth in the care you provide them until the data is corrected.

3.5.2 The Status of IHIs

Your Desktop Software product also now includes data fields related to your patients' IHI's Status, which it will keep up to date once the IHI is correctly downloaded and regularly validated. An IHI's number status will be one of the following:

Verified IHI – When an IHI has a verified status it means the HI Service Operator (DHS) has evidence of an individual's identity. If an individual enrols in the Medicare program or registers with the Department of Veterans' Affairs, Medicare Australia will automatically allocate a verified IHI if an unverified IHI does not exist.

Unverified IHI – When an IHI has an unverified status, it means the healthcare identifier was created at a healthcare facility and the individual has not provided evidence of identity to DHS.

Provisional IHI – When an IHI has a provisional status it means the identifier was created at a healthcare facility when the patient was unable to identify themselves (for example, they were unconscious). Provisional IHIs are temporary and expire after 90 days of no activity. You can update a provisional IHI to an unverified IHI or merge it with an existing verified IHI using your software system.

Note that your Desktop Software would likely only save Verified IHIs into its database. You should check this in the product's documentation. At the time of writing it is understood that the Unverified and Provisional settings are not in use due to concerns about clinical safety risks. They may be implemented at a later time as the HI Service becomes more mature.

In addition to the status of the IHI *number* (as above), the HI Service also maintains status information of the consumer's IHI *record*, as described below:

Active – an IHI is active when it does not have a date of death on the record, and the age is not greater than 130 years.

Deceased – an IHI is deceased when there is a date of death present on the record but it has not yet been matched with Fact of Death Data (FoDD) from Births, Deaths and Marriages Registries and age is not greater than 130 years.

Retired – an IHI is retired when there is a date of death present on the record and it has been matched with FoDD or has reached an age of 130 years (verified IHI records only).

Expired – an IHI is expired where it is provisional and there has been no activity on the record for 90 days, or where it is unverified and has reached an age of 130 years.

Resolved – an IHI is resolved when it has been linked with another record as part of resolving a provisional record or resolving a duplicate record, or end dated as part of the replica resolution process.

3.5.3 Options for Downloading IHIs

In terms of downloading IHIs into your system and keeping patient data up to date, there are a number of options available to you (depending on the functionality included in your Desktop Software). These are outlined below, and are not mutually exclusive:

- When a patient (existing and new) presents at your practice you may find it effective to have your reception staff, as part of the current process of verifying basic demographics, to also see if an IHI is present in their patient record. If one is not recorded the reception staff could initiate an IHI search, which your Desktop Software will be able to do.

  Note that staff who you wish to be able to perform searches and maintain IHI-related data, e.g. those at reception, will need to be setup in the HI Service as Authorised Employees, as discussed in section 3.4.7 above.

  If the software reports a match, then the IHI will be added to your patient's record.

  If the software does not report a match, it is possible that the data in your system and / or the HI Service is incorrect (see list of common matching errors above). This will need to be resolved before the patient's IHI can be downloaded, which may require the patient attending a DHS shop-front.

  Note that the inability to download an IHI does not affect in anyway the patient's right or ability to receive care or anything related to billing.

- It is possible that your Desktop Software has a feature for bulk downloading or for bulk verifying of patient IHIs. This functionality could be used as an initial step to load IHIs and also on a regular ongoing basis to check for data changes.

  Please see your Desktop Software documentation for how these features work and how to set them up if this method is of interest.

- It is probable too that your Desktop Software will allow IHIs to be directly typed in, e.g. in cases where the patient has their IHI on a letter or other official document. In these cases, the software will attempt to validate the IHI with the HI Service and will advise the user of the result.

  The same types of matching checks as discussed above are also carried out for this approach, so it is essential that data in your system matches data in the HI Service.

Having IHIs in your patient records and keeping them maintained will enable your practice to fully participate in the new national eHealth environment, including the eHealth record system, as further functionality is implemented and made available to you through updates to your Desktop Software.

3.6 Verifying Correct Operation

All the new eHealth features as they are developed and released by software suppliers are put through a rigorous conformance testing process to ensure the software is clinically safe. This includes the current updated version of your Desktop Software and any subsequent updates.

While the product is unlikely to contain faults in the new included eHealth functionality, it is still prudent to test and verify that these features operate correctly in your practice's computer environment. [35]

Both the Healthcare Identifiers and Clinical Document (CDA) Viewing features have been through a conformance testing process, which has been developed in consultation with industry and is managed by NEHTA. A summary of what's happened to make it possible for the Healthcare Identifiers functionality to be included in your Desktop Software is outlined below.

- The HI Service has undergone extensive consultation throughout the design, development and implementation stages to ensure clinical safety risks are minimised. Consultation has involved representatives from across the health sector, the vendor community, and government agencies. Representatives have provided feedback on privacy, policy and the legislative framework, functionality, integration and usability. In addition, the HI Service has been designed and built to Australian Standards;

- The software vendors have had to pass Notice of Connection (NOC) testing with DHS (as the HI Service Operator) and a Compliance, Conformance and Accreditation (CCA) testing process with a NATA accredited testing laboratory[36] in order for their products to be permitted to electronically connect to the HI Service;

- The specifications for incorporating the HI Service (and Clinical Document (CDA) Viewing) into GP Desktop Software have been developed and finalised through extensive consultation, review, testing and sign-off;

- The Desktop Software vendors and NEHTA have participated in a collaborative approach to have the products comply to those specifications; and

- In addition, the vendors own internal software quality assurance methodologies have been applied as part of their normal product development.

The sections that follow outline steps you may consider undertaking to verify the correct operation of the HI Service and Clinical Document (CDA) Viewing.

3.6.1 Healthcare Identifiers

To a large extent the HI functionality in your Desktop Software is intended to operate "under the hood" and act as a supporting function to the eHealth features that will be used more centrally in your clinical practice, e.g. e-Referrals, eHealth records, etc. Hence the approach to verification is fairly straight forward.

[35] The software update is most likely to also include other new, enhanced and/or corrected features, which you should consider also testing and verifying by whatever means you feel is appropriate.

[36] This testing has been conducted by testing laboratories that have been accredited by the National Association of Testing Authorities (NATA) specifically to perform HI testing. These laboratories are independent organisations that understand the risks associated with incorrect use of healthcare identifiers and perform tests to reduce these risks.

To proceed with the verification approach suggested in this guide, the person logged into your practice's Desktop Software will need to either:

- Have a HPI-I and be registered with the HI Service, or
- Be registered in the HI Service as an Authorised Employee.

Suggested steps include:

1. In your Desktop Software, ensure that your practice's HPI-O is recorded accurately.

2. Select and view a patient record that:
   a) Does not have an IHI recorded against it, and
   b) Has been recently used in an electronic transaction with DHS,

3. Check that data entered in the following fields appears to be valid:
   - Medicare Card number or DVA number
   - Surname
   - Given Name
   - Date of Birth
   - Gender
   - Address

4. Use the function in your Desktop Software to find the patient's IHI.

5. If the software reports the result as successful:
   - Check that the patient's IHI data field contains 16 digits and that the IHI Status fields show the IHI as being "verified".

6. If the result is not successful, there may be a number of reasons why an exact match is not possible:
   - The practice may need to review the data it holds to determine currency (e.g. patient change of name) and accuracy (e.g. Medicare card number recorded correctly). This can be checked with the patient at their next visit and updates made to the data in your Desktop Software.
   - The patient may not have renewed their current details with DHS. It would be helpful to advise the patient to contact DHS to have their data checked and updated.
   - You may need to check that the practice software has been correctly installed.

When you have successfully downloaded a patient's IHI into your Desktop Software system, you can be confident that your software update has been successfully installed.

3.6.2 Clinical Document (CDA) Viewing

The CDA document viewing feature should be verified when your Desktop Software is capable of receiving such documents. The vendor can advise you when this capability will be included in their product.

In addition, as other healthcare organisations gain the ability to create and send CDA documents, e.g. discharge summaries from nearby hospitals, they will need to work with their community of healthcare providers to ensure that these are implemented safely and correctly.

3.7 Achieving Meaningful Use

The benefits to your practice of implementing the new eHealth features in this updated version of your Desktop Software, as outlined in this User Guide, relate mainly to:

- Enhancing clinical governance arrangements and your practice's approach to quality improvement; and

- Establishing the essential foundations, in terms of staff roles, work processes, data quality and technologies that will enable your practice to implement further national eHealth features, including the eHealth record system, as they are released.

The subsequent eHealth features will utilise what you have now implemented and enable you to conduct a wide range of clinically meaningful transactions more efficiently, more accurately and more safely. Importantly the national eHealth system will assist with "closing the loop" on many, e.g. for referrals with specialist letters and for matching prescriptions with dispensing records.

4 Checklists for HI Usage

The following information is provided to assist you, other clinicians and practice staff remember the key things that need to be done in relation to using the Healthcare Identifiers Service in your day to day activities, assuming it has been all set up and verified as outlined in this User Guide.

4.1 For Front-Desk and Practice Administration Roles

Patient Contact Information and their IHI

☐ 1. To interact with the HI Service for managing patient identification information, you need have a registered HPI-I or be an Authorised Employee.

- Note that searching for an IHI should only be done when required as part of providing healthcare, and that an audit record is stored of HI Service uses.

☐ 2. As part of reviewing with a new or existing patient their demographic and Medicare details in your Desktop Software:

☐ 2.1 If an IHI exists in their record, then proceed to your next normal step in the process you are performing.

☐ 2.2 Otherwise check:

i. That the Medicare/DVA card number is correct
ii. That the Surname and Given Name(s) are the same as on the Medicare/DVA card
iii. Date of Birth
iv. Gender
v. Address

☐ 2.3 When this data is entered, use the feature in your Desktop Software to download the patient's IHI.

☐ 2.4 If this is successful, then proceed to your next normal step in the process you are performing.

☐ 2.5 Otherwise:

i. There is a mismatch of the above data between what the patient has advised and what is stored in the HI Service.
ii. The patient will need to contact DHS to resolve the error(s). They should try and correct their data through calling DHS or through its online services. Depending on the error, they may need to go to a DHS shop-front.
iii. The patient's visit with the Doctor can proceed without any limitation, except that many eHealth activities cannot be conducted.

Changes in Organisation and Staff

- The OMO in your practice is required to maintain records in the HI Service for:
    - The practice organisation (HPI-O)
    - Links with clinician's HPI-Is
    - The Healthcare Provider Directory (HPD)
    - Authorised Employees (which may be lodged in a spread-sheet to the HI Service Operator).
- When any such information changes, you need to advise the OMO promptly so that the data in the HI Service can be updated.
- Note that having two OMOs removes reliance on one person to keep records up to date in a timely fashion.

4.2 For GPs and Other Clinicians

As the HI Service is intended to mostly operate "under the hood" and assuming the practice's front-desk or administration staff manage patient IHIs, there is not a lot that clinicians need to concern themselves about the HI Service on a day to day basis. It is acknowledged that this may not be the case for practices that do not have non-clinical staff.

Key responsibilities for GPs and other clinicians include:

- ☐ 1. Obtain your HPI-I and provide it to the OMO (e.g. Practice Manager) of the healthcare organisations in which you work.
- ☐ 2. Make sure you have and maintain an Individual PKI certificate and that the OMO(s) of healthcare organisations in which you work know of it. Be sure to remember your certificate's password.
- ☐ 3. As per good practice, ensure the entry in your Desktop Software of complete and accurate clinical data for your patients. This is especially important for medical histories, allergies, medications and immunisations.
- ☐ 4. If your contact or professional information changes, then you need to login to the AHPRA web-site promptly and update the pertinent information. This data will then be updated in DHS's systems, including in the HI Service, and the Healthcare Provider Directory (HPD), depending on what data has been consented for viewing. You should also check the HPD to ensure the correct details are displayed.
- ☐ 5. You should login into DHS's HPOS web-site to view and verify information related to your HPI-I and how your information is displayed in the HPD (so that other healthcare providers can accurately identify you when they search it). Note you must provide your consent for your information to appear in the HPD via the appropriate form.
- ☐ 6. You may use the HPD to search for healthcare providers relevant to the care of your patients, e.g. for a referrals or general advice.

5 Further Information and Support

The following table lists how you might go about addressing a range of support requirements related to implementing the eHealth features presented in this User Guide.

Requirement	Suggested Source
Specifically about your Desktop Software product	The product's Vendor
The Healthcare Identifier Service provided by DHS, and for DHS-related PKI, security, access and other aspects	http://www.medicareaustralia.gov.au/provider/ Healthcare Identifiers (HI) Service online user guide: http://www.medicareaustralia.gov.au/hpos/online-user-guides/hi/ Feedback or Complaints can be provided online or via email. For online go to: www.humanservices.gov.au > Feedback > Customer Feedback; Specifically for the HI Service, an email can be sent to: healthcareidentifiers@humanservices.gov.au Phone: 1300 361 457
eHealth programs in your Local Area, including related to clinical governance and quality improvement	Your Medicare Local or Division of General Practice Your Local Health Network
eHealth Contacts for AGPN (to be known as AMLN from 1 July 2012)	http://agpn.com.au/programs/ehealth-and-information-management/ehealth-program-contacts

6 Acronyms and Abbreviations

Acronym	Meaning
ACSQHC	Australian Commission on Safety and Quality in Healthcare
AGPN	Australian General Practice Network – from 1 July 2012 to be known as Australian Medicare Local Network
AHPRA	Australian Health Practitioner Regulation Agency
AMA	Australian Medical Association
AMLN	Australian Medicare Local Network
CDA	Clinical Document Architecture
CDSA	Clinical Data Self Assessment
DHS	Commonwealth Department of Human Services, formally known as Medicare
DoHA	Commonwealth Department of Health & Ageing
DAO	Duly Authorised Officer
GP	General Practitioner
HI	Healthcare Identifiers
HI Service	Healthcare Identifiers Service
HI Service Operator	Commonwealth Department of Human Services (DHS)
HL7	Health Level Seven
HPD	Healthcare Provider Directory
HPI-I	Healthcare Provider Identifier – Individual
HPI-O	Healthcare Provider Identifier – Organisation
HPOS	Health Professional Online Services
IHI	Individual Healthcare Identifier
LHN	Local Health Network
ML	Medicare Local
NASH	National Authentication Service for Health
NEHTA	National E-Health Transition Authority
OMO	Organisation Maintenance Officer
PCEHR	Personally Controlled Electronic Health Record, now known as National Electronic Health Record
PKI	Public Key Infrastructure
RO	Responsible Officer
SHS	Shared Health Summary
SMD	Secure Message Delivery
RACGP	Royal Australian College of General Practitioners

nehta
eHealth